Daily Open Source Infrastructure Report
01 October 2015

Top Stories

- Officials released findings on a November 2014 toxic chemical leak at a DuPont plant in Texas and found that that a combination of building, maintenance, and human errors led to the release of nearly 24,000 pounds of methyl mercaptan. – *KPRC 2 Houston* (See item **4**)

- Ford Motor Company issued recalls September 30 for approximately 380,000 model year 1998 – 2016 vehicles due to various compliance and mechanical issues. – *WWJ 62 Detroit* (See item **5**)

- Thirteen manufacturers and distributors issued recalls September 29 for about 1.3 million bicycles due to an issue which could stop the front wheel abruptly or separate it from the bicycle. – *U.S. Consumer Product Safety Commission* (See item **6**)

- Proofpoint published research revealing that the Dyreza trojan has been used to phish information technology (IT) supply chain credentials for up to 20 organizations. – *Threatpost* (See item **25**)

Fast Jump Menu

PRODUCTION INDUSTRIES
- Energy
- Chemical
- Nuclear Reactors, Materials, and Waste
- Critical Manufacturing
- Defense Industrial Base
- Dams

SUSTENANCE and HEALTH
- Food and Agriculture
- Water and Wastewater Systems
- Healthcare and Public Health

SERVICE INDUSTRIES
- Financial Services
- Transportation Systems
- Information Technology
- Communications
- Commercial Facilities

FEDERAL and STATE
- Government Facilities
- Emergency Services

Energy Sector

1. *September 30, U.S. Environmental Protection Agency* – (Massachusetts) **EPA settlement ensures that Ludlow, Mass. water is better protected from oil spills.** The U.S. Environmental Protection Agency announced September 30 that Buckeye Pipe Line Co., will pay a $78,780 penalty to resolve claims that it violated Federal oil spill prevention regulations following an inspection of an oil storage facility in Ludlow, Massachusetts, revealed that the company's oil spill prevention plan was deficient in several areas and had failed to have adequately sized containment for one of its oil tanks. The company took steps to ensure that the plan was updated and completed all necessary containment work in July.
Source: http://yosemite.epa.gov/opa/admpress.nsf/0/FD73646E0E69650685257ECF00606ACA

2. *September 29, Associated Press* – (National) **EPA sets stricter emission standards for oil refineries.** The U.S. Environmental Protection Agency announced September 29 that new rules were enacted to help reduce toxic pollution from oil refineries, which include forcing operators to adopt new technology that better monitors and controls emissions, the installation of air monitors along fence lines, and the monitoring of levels of benzene and other dangerous pollutants.
Source: http://www.mercurynews.com/california/ci_28893817/epa-set-tighten-smog-limits-business-gears-fight

3. *September 29, WMBF 32 Myrtle Beach* – (North Carolina) **Duke Energy to pay seven million settlement for groundwater violations.** Duke Energy reached a $7 million settlement September 29 with the North Carolina Department of Environmental Quality regarding alleged groundwater violations at the company's retired Steam Electric plant in Wilmington and a second facility in the State. The settlement will resolve former, current, and future groundwater issues at all 14 coal facilities in the State.
Source: http://www.wmbfnews.com/story/30142341/duke-energy-to-pay-seven-million-settlement-for-groundwater-violations

Chemical Industry Sector

4. *September 30, KPRC 2 Houston* – (Texas) **Report finds series of errors caused deadly DuPont plant accident in La Porte.** The U.S. Chemical Safety Board (CSB) released findings from an interim investigation into a November 2014 toxic chemical leak at a DuPont manufacturing plant in La Porte which killed 4 employees, revealing that the chain of events leading up to the incident was set in motion 5 days prior, when a water dilution system was inadvertently activated, and that a combination of building, maintenance, and human errors led to the release of nearly 24,000 pounds of methyl mercaptan. CSB made seven safety recommendations, including a comprehensive engineering analysis of the building along with safer design options to be reported to the agency.
Source: http://www.click2houston.com/news/dupont-to-speak-on-deadly-chemical-leak-near-la-porte/35571142

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

5. *September 30, WWJ 62 Detroit* (National) **Ford issues six separate recalls for 380K vans, trucks, SUVs, and cars.** Ford Motor Company issued recalls September 30 for approximately 340,000 model years 1998 – 2003 Windstar minivans due to potential risks of corrosion and cracking in vehicle axles, about 37,000 model year 2015 F-150 trucks due to an issue with the vehicle's adaptive cruise control system that could cause it to engage its automatic brakes and collision warning system when passing large, highly reflective trucks, and about 1,500 model year 2016 F-53 and F-59 stripped chassis vehicles due to a potential issue with the vehicles' shift brackets which could allow shifting into reverse without braking. The announcement included recalls for more than 1,000 additional vehicles due to various compliance and mechanical issues.
Source: http://detroit.cbslocal.com/2015/09/30/ford-issues-six-separate-recalls-for-380k-vans-trucks-suvs-and-cars/

6. *September 29, U.S. Consumer Product Safety Commission* – (National) **Thirteen manufacturers, distributors recall bicycles with front disc brakes to replace quick release lever due to crash hazard.** Thirteen manufacturers and distributors issued recalls September 29 for about 1.3 million bicycles in the U.S. equipped with front disc brakes and quick release levers due to an issue which could cause an open quick release lever to contact the front disc brake rotor, stopping the front wheel abruptly or separating it from the bicycle. The products were sold at various retailers nationwide from 1998 – 2015.
Source: http://www.cpsc.gov/en/Recalls/2015/Thirteen-Manufacturers-Distributors-Recall-Bicycles-with-Front-Disc-Brakes-to-Replace-Quick-Release-Lever/?utm

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

7. *September 30, U.S. Securities and Exchange Commission* – (National) **SEC sanctions 22 underwriting firms for fraudulent municipal bond offerings.** The U.S. Securities and Exchange Commission announced enforcement actions September 30 against 22 municipal underwriting firms under the Municipalities Continuing Disclosure Cooperation (MCDC) Initiative, reportedly finding that the firms violated Federal securities laws by selling municipal bonds using offering documents containing materially false statements or omissions regarding the bond issuers' compliance with disclosure obligations. The underwriting firms agreed to cease all operations of such violations and pay civil penalties.
Source: http://www.sec.gov/news/pressrelease/2015-220.html

8. *September 29, WBBM 2 Chicago* – (Illinois) **FBI searching for 'North Center Bandit.'** The FBI is searching for information leading to the arrest of a suspect dubbed the "North Center Bandit," who allegedly robbed 3 bank branches in North Center from August 21 – September 25.
   Source: http://chicago.cbslocal.com/2015/09/29/fbi-searching-for-north-center-bandit/

Transportation Systems Sector

9. *September 30, WISN 12 Milwaukee* – (Wisconsin) **St. Francis intersections reopen after train collision.** Crews worked to clear the tracks after two Union Pacific trains collided, closing an intersection in St. Francis September 29 after a train carrying rail was derailed from the tracks. The incident remains under investigation.
   Source: http://www.wisn.com/news/train-blocking-intersections-in-st-francis/35566256

10. *September 29, Allentown Morning Call* – (Pennsylvania) **I-78 trucks burst into flames in Berks crash, seriously injuring 1 man.** Interstate 78 in Berks County was shut down for several hours September 29 while crews responded to the scene of a 4-vehicle accident that occurred in a construction area and injured 2 people.
    Source: http://www.mcall.com/news/traffic/mc-tractortrailer-accident-closes-i78-20150929-story.html

11. *September 29, WISH 8 Indianapolis* – (Indiana) **4 semis collide on I-65 in southern Indiana.** Interstate 65 northbound in Johnson County, Indiana, near mile marker 86.5 was shut down for several hours September 29 while crews responded to an accident that involved 4 semi-trucks. No injuries were reported.
    Source: http://wlfi.com/2015/09/29/4-semis-collide-on-i-65-in-southern-indiana/

Food and Agriculture Sector

12. *September 30, U.S Department of Agriculture* – (California) **Royal Frozen Food recalls frozen food products produced without a fully implemented HACCP plan, containing an undeclared allergen, and missing the mark of inspection.** The Food and Safety and Inspection Service reported September 29 that Los Angeles-based Royal Frozen Food issued a recall for approximately 230 pounds of its frozen beef and pork products that were not produced under a fully implemented Hazard Analysis and Critical Control Points plan, contained undeclared egg, and were distributed without the Federal mark of inspection.
    Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2015/recall-126-2015-release

13. *September 29, U.S. Department of Labor* – (Ohio) **Teen contractor loses leg, co-worker loses fingers at Case Farms.** The Occupational Safety and Health Administration (OSHA) cited Case Farms Processing Inc., September 29 for 2 willful, 10 repeated, and 4 serious safety violations at the company's Canton facility for exposing workers to amputation, fall, electrical, and other serious hazards after 2 workers suffered injuries. OSHA levied proposed penalties of $424,600 against the

company and $179,700 against its owner.
https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=28803

14. *September 29, Food Poison Journal* – (National) **Salmonella cucumber outbreak jumps to 671 sick, 131 hospitalized, 3 dead.** The U.S. Centers for Disease Control and Prevention and U.S. Food and Drug Administration reported September 29 that the total number of people affected in an ongoing multistate Salmonella Poona outbreak rose to 671 cases across 34 States, an increase of 113 cases since September 22. Authorities are investigating the outbreak which is believed to be tied to cucumbers imported from Mexico.
Source: http://www.foodpoisonjournal.com/foodborne-illness-outbreaks/salmonella-cucumber-outbreak-jumps-to-671-sick-131-hospitalized-3-dead/#.VgwE2MtVikq

Water and Wastewater Systems Sector

See item **1**

Healthcare and Public Health Sector

15. *September 29, WDIV 4 Detroit* – (Michigan) **14 patients diagnosed with salmonella at Henry Ford Hospital.** Hospital officials are investigating the cause of Salmonella outbreak that infected more than a dozen patients at Henry Ford Hospital in Detroit the week of September 21.
Source: http://www.clickondetroit.com/news/14-patients-diagnosed-with-salmonella-at-henry-ford-hospital/35566506

For another story, see item **29**

Government Facilities Sector

16. *September 30, Softpedia* – (New Jersey) **Despite new equipment, Rutgers University goes down after DDoS attack.** Rutgers University announced September 28 that the university experienced network issues due to a distributed-denial-of-service (DDoS) attack, which limited access to the Internet for several hours. The attack was allegedly orchestrated by a hacker known as Exfocus, and followed four previous attacks against the university between March and May.
Source: http://news.softpedia.com/news/despite-new-equipment-rutgers-university-goes-down-after-ddos-attack-493155.shtml

17. *September 30, Staten Island Advance* – (New York) **College of Staten Island closed due to power outage.** A campus-wide power outage caused by a failure of an electrical substation prompted the closure of the College of Staten Island in New York September 30.
Source: http://www.silive.com/northshore/index.ssf/2015/09/college_of_staten_island_close.html

18. *September 30, NJ.com* – (New Jersey) **Hughes Justice Complex in Trenton**

evacuated due to Freon leak. A Freon leak prompted the evacuation of the Richard J. Hughes Justice Complex in Trenton September 30. The building remains closed while crews pump fresh air into the facility, and will reopen once officials clear the scene.
Source: http://www.nj.com/mercer/index.ssf/2015/09/hughes_justice_complex_in_trenton_evacuated_due_to.html

19. *September 29, WTOC 11 Savannah* – (Georgia) **12-year-old in police custody accused of making bomb threats in Bulloch Co.** Police took a juvenile into custody in connection to a series of phoned bomb threats that forced the evacuation and closure of four Bulloch County schools September 29.
Source: http://www.wtoc.com/story/30142534/4-bulloch-co-schools-evacuated-due-to-bomb-threats

20. *September 29, Albany Times Union* – (New York) **Police: Skidmore employee stole $258k in gadgets from college.** A former employee at Skidmore College in Saratoga Springs was arrested September 28 for allegedly stealing over $258,000 worth of computers, cameras, smart phones, and other electronics from the college by using a college credit card and shipping the items to his home. The school has since implemented stricter internal controls and updated its purchase approval procedures.
Source: http://www.timesunion.com/local/article/Police-Skidmore-employee-stole-258k-in-gadgets-6537953.php

21. *September 29, WCNC 36 Charlotte* – (North Carolina) **7 Lake Norman HS students charged for computer breach.** Iredell Sheriff's Office announced September 29 that at least 7 Lake Norman High School students were arrested and charged for allegedly manipulating a school-issued laptop and gaining administrative access to more than 33 other students' computers, allowing the individuals to control the computer's functions. Officials do not believe that any personal data, testing materials, or grades were compromised.
Source: http://www.wcnc.com/story/news/crime/2015/09/29/7-lake-norman-hs-students-charged-for-computer-breach/73025436/

For another story, see item **27**

Emergency Services Sector

Nothing to report

Information Technology Sector

22. *September 30, Help Net Security* – (International) **Scammers use Google AdWords, fake Windows BSOD to steal money from users.** Security researchers from Malwarebytes discovered that cybercriminals are using Google's AdWords to place malicious links at the top of Google's search page for common searches, which would lead to a fake "Blue Screen of Death" (BSOD) page prompting users to call a toll-free "helpline" with scammers that would solicit payments for support services and personal and bank account information.

Source: http://www.net-security.org/secworld.php?id=18913

23. *September 30, Softpedia* – (International) **Microsoft Exchange Server fixed against information disclosure bug.** Microsoft released an update for Exchange Server 2013 addressing a vulnerability in Outlook Web Access (OWA) that could allow an attacker to gain access to an active Webmail session by forcing Exchange Server to dump debug data via a maliciously crafted Uniform Resource Locator (URL), granting access to previously inaccessible cookie session information.
Source: http://news.softpedia.com/news/microsoft-exchange-server-fixed-against-information-disclosure-bug-493157.shtml

24. *September 30, Threatpost* – (International) **Apple Gatekeeper bypass opens door for malicious code.** Security researchers from Synack discovered that Apple's Gatekeeper security platform could be bypassed by tricking a user into downloading a signed and infected application from a third-party source, or by loading a malicious library over an insecure HyperText Transfer Protocol (HTTP) download via a man-in-the-middle (MitM) position to gain access to the system.
Source: https://threatpost.com/apple-gatekeeper-bypass-opens-door-for-malicious-code/114851/

25. *September 29, Threatpost* – (International) **Dyreza trojan targeting IT supply chain credentials.** Security researchers from Proofpoint published research revealing that the Dyreza trojan has been used to phish information technology (IT) supply chain credentials for up to 20 organizations, including software companies supporting fulfillment and warehousing, and computer distributors. Researchers believe that hackers intend to infect all points of the supply chain to possibly divert physical shipments, issue payments and invoices to artificial companies, or enact large-scale gift-card issuances.
Source: https://threatpost.com/dyreza-trojan-targeting-it-supply-chain-credentials/114836/

26. *September 29, Threatpost* – (International) **SAP patches 12 SQL injection, XSS vulnerabilities in HANA.** SAP released updates addressing 12 structured query language (SQL), cross-site scripting (XSS), and memory corruption vulnerabilities in its HANA in-memory management system that could allow an attacker to abuse management interfaces and compromise stored information, or lock users out of the platform, among other exploits.
Source: https://threatpost.com/sap-patches-12-sql-injection-xss-vulnerabilities-in-hana/114840/

27. *September 29, Securityweek* – (International) **Linux XOR DDoS botnet flexes muscles with 150+ Gbps attacks.** Security researchers from Akamai Technologies released details of a botnet targeting primarily corporations in Asia that is capable of launching 150+ gigabit-per-second (Gbps) distributed denial-of-service (DDoS) attacks from Linux systems compromised by the XOR DDoS trojan, as well as being able to download and execute arbitrary code and self-update.

Source: http://www.securityweek.com/linux-xor-ddos-botnet-flexes-muscles-150-gbps-attacks

For another story, see item **16**

Communications Sector

Nothing to report

Commercial Facilities Sector

28. *September 30, WNBC 4 New York City* – (New York) **'Suspicious' fire takes out steeple at Staten Island church: Fire officials.** Authorities are investigating a 3-alarm fire at Casa de Milagros (House of Miracles) on Staten Island that broke out September 30 and prompted the response of more than 100 firefighters. One firefighter was injured and officials deemed the fire as "suspicious."
Source: http://www.nbcnewyork.com/news/local/Massive-Fire-Takes-Out-Steeple-at-Staten-Island-Church-Fire-Officials-330056531.html

29. *September 29, WCBS 2 New York City* – (New York) **More cases of Legionnaires' disease diagnosed in the Bronx; 7 cooling towers test positive.** New York City health officials reported September 29 that there are 10 reported cases of Legionnaires' disease linked to a cluster in Morris Park, and that 7 cooling towers in the Bronx area tested positive for the Legionella bacteria. Officials ordered all seven locations to be cleaned and disinfected.
Source: http://newyork.cbslocal.com/2015/09/29/morris-park-legionnaires-disease/

30. *September 29, Jersey Journal* – (New Jersey) **37 people displaced by suspicious Jersey City fire off McGinley Square.** A 3-alarm fire September 29 at an apartment building near Jersey City's McGinley Square displaced 37 residents, and was deemed suspicious after authorities determined that the blaze began at a vacant building that is attached the apartment complex.
Source: http://www.nj.com/hudson/index.ssf/2015/09/34_people_displaced_by_jersey_city_fire_this_morni.html#incart_river

Dams Sector

Nothing to report

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.